



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10003257 A**(43) Date of publication of application: **06 . 01 . 98**

(51) Int. Cl.

G09C 1/00**G06F 1/00****G06F 17/60****H04L 9/32**(21) Application number: **08156964**(22) Date of filing: **18 . 06 . 96**(71) Applicant: **TOSHIBA CORP**(72) Inventor: **KOGANEZAWA YUICHI
KITAORI MASASHI**(54) **METHOD AND DEVICE FOR ADDING
ELECTRONIC SIGNATURE, AND METHOD FOR
VERIFYING ELECTRONIC SIGNATURE**

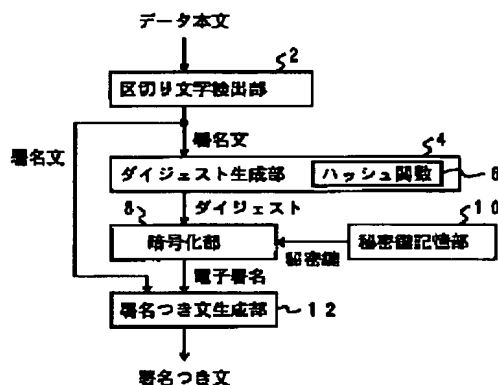
(57) Abstract:

PROBLEM TO BE SOLVED: To extract and quote the pair of a signed sentence/an electronic signature from an electronic document by adding the electronic signature against a data main sentence in a signature sentence unit.

SOLUTION: This electronic signature adding device is provided in the terminal device of the transmitter side and consists of a segmenting character detecting section 2, a digest generating section 4, a ciphering section 8, a secret key storage section 10 and a signed sentence generating section 12. When the signature information is added to the electronic sentence to prove that the sentence is written by the person who made the signature, the electronic sentence is divided into plural signed sentences using a beforehand decided specific character or a specific character column which appear in the sentence as a segment, signature information is generated based on the signed sentences for every divided signed sentence and the signature information is stored in accordance with the signed sentences. In other words, the electronic sentence, which is the signature object, is divided into plural signed sentences and an electronic signature is added to

a signature sentence unit. Note that the specific character is at least one of a blank character, punctuation characters and parenthesis characters.

COPYRIGHT: (C)1998,JPO



Best Available Copy

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-3257

(43) 公開日 平成10年(1998) 1月6日

(51) Int.Cl. ⁶	識別記号	片内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 4 0	7259-5 J 7259-5 J	G 0 9 C 1/00	6 4 0 B 6 4 0 D
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 E
	17/60		15/21	Z
H 0 4 L 9/32			H 0 4 L 9/00	6 7 5 B

審査請求 未請求 請求項の数10 O L (全 17 頁)

(21) 出願番号 特願平8-156964

(22) 出願日 平成8年(1996) 6月18日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 小金澤 雄一

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 北折 昌司

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

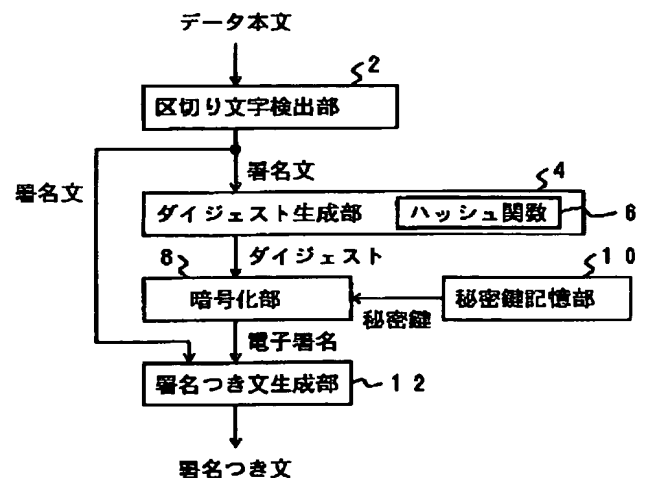
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 電子署名付加方法及び電子署名装置並びに電子署名検証方法

(57) 【要約】

【課題】 電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする電子署名装置を提供すること。

【解決手段】 電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割し、分割された署名文ごとに、該署名文をもとに署名情報を生成し、前記署名文に対応付けて前記署名情報を格納することを特徴とする。



【特許請求の範囲】

【請求項 1】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割し、分割された署名文ごとに、該署名文をもとに署名情報を生成し、前記署名文に対応付けて前記署名情報を格納することを特徴とする電子署名付加方法。

【請求項 2】前記特定文字は、空白文字、句点文字、読点文字または括弧文字のうちの少なくとも 1 つであることを特徴とする請求項 1 に記載の電子署名付加方法。

【請求項 3】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、署名情報を付加する対象となる文書中から予め定められた特定文字を除外し、前記文書中から前記特定文字を除外して得られた文をもとに署名情報を生成し、前記署名情報を付加する対象となる文書に、生成された前記署名情報を付加することを特徴とする電子署名付加方法。

【請求項 4】前記特定文字は、空白文字、句点文字、読点文字、括弧文字および印刷不可能な制御文字のうちの少なくとも 1 つであることを特徴とする請求項 3 に記載の電子署名付加方法。

【請求項 5】前記署名情報は、該署名情報のもととなる文から所定のハッシュ関数を用いて生成したダイジェストを公開鍵暗号方式の所定の秘密鍵で暗号化したものであることを特徴とする請求項 1 または 3 に記載の電子署名付加方法。

【請求項 6】前記署名情報は、該署名情報による署名対象となる文の前方または後方に挿入することを特徴とする請求項 1 または 3 に記載の電子署名付加方法。

【請求項 7】作者を証明する署名情報が付加された電子化された文書を受け取り、受け取った前記文書中の印字可能文字の総数と印字不可能文字の総数をもとに所定の計算式を用いて前記署名情報の信頼性を評価することを特徴とする電子署名検証方法。

【請求項 8】前記特定文字は、印刷不可能な文字であることを特徴とする請求項 7 に記載の電子署名検証方法。

【請求項 9】前記所定の計算式は、 p を印字不可能文字の種類、 m を文書の文字数、 k を印字不可能な文字の数、 l をメッセージダイジェストのビット長、信頼性の値を T としたとき、 $T = (p^k) \times (m + 1) \times (m + 2) \times \dots \times (m + k) / (2^l)$ で表されるものであり、求められた信頼性の値 T と予め定められたしきい値とを比較することにより前記署名情報の信頼性を評価することを特徴とする請求項 7 に記載の電子署名検証方

法。

【請求項 10】電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名装置において、電子化された文書を、該文書中に出現する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割する手段と、分割された署名文ごとに、該署名文をもとに署名情報を生成する手段と、前記署名文に対応付けて前記署名情報を格納する手段とを備えたことを特徴とする電子署名装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子化された文書データの送信・蓄積にあたって改ざんを防止するために作者を証明する署名データを該文書データに付加する電子署名付加方法及び電子署名装置、並びに電子署名の付加された電子化文書データの信頼性を評価する電子署名検証方法に関する。

【0002】

【従来の技術】近年では、電子メールに代表されるように文書情報を電子化して（コード化して）送受信するような情報システムが広く普及している。受信された電子化文書情報は、通常、磁気記録媒体等に蓄積され、文書情報の一部を引用するなどの再利用をすることもできる。

【0003】ところで、一般的に文書は、閲覧可能な者を限定する必要がある内容のものと、閲覧可能な者を不特定とする内容のものとに分けることができる。例えば、個々の企業や人の秘密に関するものを内容とする電子化文書情報が前者に該当するであろうし、企業や人あるいは公共機関などが第三者に知らせたい事柄に関するものを内容とする電子化文書情報が後者に該当するであろう。前者に該当する電子化文書情報は、例えば暗号化しておくことにより復号鍵を持たない者には内容を知られないようにすることができる。一方、後者に該当する電子化文書情報は、通常、平文のままで、誰でもアクセスできるようにされる。

【0004】ここで、後者に該当する電子化文書情報は、その性質上から通常は平文であるため、不正に内容を改ざんされる危険性がある。特に、公的な情報（電子化された情報）はデマや意図的な情報操作の標的になり易く、万一、こうした不正が行われた場合の社会的影響は甚大であると考えられる。

【0005】そこで、必要に応じて電子化文書には、その内容が改ざんされていないことなどを証明する電子署名データが付加される。この電子署名データにより、例えば「その電子化文書は確かに公共機関が作成したものであって不正に改ざんされた情報やデマではない」ことが証明される。

【0006】以下では、電子メールを例にして電子署名

の原理を説明する。図19に、従来の電子署名を適用した電子メールの処理の流れを示す。

(1) 送信側では、データ本文を受信者に送る場合、データ本文を圧縮してダイジェスト(圧縮文)を生成し、このダイジェストを送信側の持つ秘密鍵で暗号化してデジタル署名と呼ばれるデータ(圧縮暗号文)を生成し、これをデータ本文に付加して送信する。

【0007】(2) 受信側では、データ本文に付加されたデジタル署名データを送信側の持つ秘密鍵に対応する公開鍵で復号して、もとのダイジェスト・データを生成するとともに、受信したデータ本文を圧縮してダイジェスト・データを生成する。そして、生成した2つのダイジェスト・データを比較することによって、データ本文が正しいかどうかを判定することができる。

【0008】このように電子署名は、(1) 情報が改変されておらず、原情報のまま正しいものであることを保証するメッセージ認証の機能と、(2) 情報の生成・伝送・処理・記憶・判断などの行為に関与した実体A(エンティティA、例えばAという人)が、そのエンティティAであることを保証する機能であるエンティティ認証との両方の機能を持つものである。

【0009】すなわち、エンティティAとBの間で、作成者をAとする情報について何らかの問題が発生した場合に、(1) 問題となっているメッセージの送り主が確かにAであることをB側で証明できる機能を持ち、またBがその事実を明示する証拠を呈示することができ、かつ、(2) Bが「にせ」のメッセージを偽造して、「そのメッセージの送り主がAである」と主張することができないことをいう。

【0010】次に、図20を参照しながら、送信側での*

X, Y : データブロック。算術モジュロより小さい。
n : 算術モジュロ
e : 公開指数
d : 秘密指数
p, q : 素数。この積が算術モジュロ(n)となる。
lcm : 最小公倍数
mod n : 算術モジュロn

を用いて、この非対称アルゴリズムは、次のような、データブロックの転送のための指数関数を使用する。

$$Y = X^e \text{ mod } n \quad (\text{ただし、} 0 \leq X < n) \quad 40$$

$$X = Y^d \text{ mod } n \quad (\text{ただし、} 0 \leq Y < n)$$

例えば、これは下記の解によって満足される。

$$e d \text{ mod } lcm(p-1, q-1) = 1 \quad \text{または} \\ e d \text{ mod } (p-1)(q-1) = 1$$

この処理を有効にするために、データブロックは整数と解釈されなくてはならない。

【0015】ここで、公開されるのは(e, n)であり、秘密鍵はdである。署名では秘密鍵dを使ってダイジェストが暗号化される。誰でもダイジェストを生成することはできるが、公開されている(e, n)から秘密

* 署名データの生成手順についてより詳しく説明する。まず、署名対象となる本文全体1001は、ハッシュ関数1002と呼ばれる変換処理によって圧縮文1003すなわちダイジェスト1003となる。

【0011】ここで、ハッシュ関数とは、任意長のデジタルデータを一定長のデジタルデータに変換する一方向性関数であり、変換後のデータからもとのデータを推定することが極めて困難な点と、変換後のデータが予測困難な乱数である点に特徴がある。これによって、長いデジタルデータの全てを暗号化により署名する必要はなく、ハッシュ関数が生成した一定長のデジタルデータすなわちメッセージダイジェストを暗号化しさえすれば、全体のデータに署名したのと等価な効果が期待できるものである。良く用いられているハッシュ関数としてはMD5(参考文献: RFC1321 The MD5 Message-Digest Algorithm)があげられる。

【0012】次に、ダイジェスト1003は本人だけが知る情報を鍵1004として暗号化される。ここで使われるのが非対称鍵暗号方式の秘密鍵であり、なかでもRSA方式が良く用いられる。

【0013】上記のようにして生成された署名1005は、本文とともに送信され(図中106)、受信側で検証されることになる。ここで、上記のRSA方式について簡単に説明する。

【0014】RSAは、R. L. Rivest, A. Shamir, L. Adlemanによって考案されたシステムで、この手法はモジュロ指数に依存している。公開指数と算術モジュロからなるパラメータ対を公開鍵、秘密指数と算術モジュロからなるパラメータ対を秘密鍵と呼び、以下の記号および略号

鍵dを導くことは非常に困難であるため、署名は秘密鍵dを知る本人だけが事実上行うことができる。しかるに、(e, n)は公開されており、これらが上記所定の計算式を満たす関係にあることから、誰でも暗号を解くことが可能となり、署名を検証することができるのである。

【0016】次に、図21を参照しながら、受信側での署名検証の手順についてより詳しく説明する。受信側では、受け取った署名つき文1006中の本文から所定のハッシュ関数1002によりダイジェスト1(図中1011)を生成する。一方、本文に添付された署名をRSA公開鍵1010を用いて暗号を解くことによって、本文の著者である本人が生成した圧縮文であるダイジェス

ト2（図中1012）を作り出す。そして、両者の一致を見ることによって（1013）、一致していれば本文が署名を作った人物によって作られた文章であることが示され（1014）、また一致していなければ署名が間違っている、すなわち誰かが改ざんしたことを検出することが可能となる（1015）。

【0017】このように電子署名は文章の改ざんを防止し、文章の内容の信頼性を保つことができる。しかしながら、上記のような従来の電子署名は文章全体に対して行われるため、文章全体からある文を部分的に引用した場合、電子署名はその部分に対して全く役にたたなくなってしまうという問題点があった。特に、引用された部分が意味のある重要なものである場合、改ざんの有無等を検出できないことは非常に不都合である。

【0018】より具体的に説明すると、例えば図22に示めされるように、Aが作成した文1、文2、文3からなる文章全体に電子署名Xを付加してBに転送したとする。その後、BがAにより作成された文章中から文2のみを引用して、文a、文2、文bからなる文章を作成し、これに電子署名Yを付加してCに転送したとする

（ここで、文a中に、文2の作成者はAであることが書かれていたものとする）。この場合、Cにとっては、Bの言う通り本当に文2の作成者がAであるのか否かについて認証不能となる。

【0019】また、上記のような不都合を回避するためには、例えば上記の具体例で言うと、Bは文2だけをCに転送するために、文1、文2、文3からなる文章全体とその電子署名を転送する必要がある、非常に不都合である。

【0020】一方、上記のような引用については他の問題点がある。すなわち、例えば文章全体を引用した際に、編集等の結果として空白や改行といった文書の意味に関与しない制御文字が意識しないところで挿入された場合、あるいは印刷により印字できない文字を含んでいる場合のように、意図しない改ざんが行われたような場合、文書の意味は全く変えられていないにもかかわらず、従来の電子署名メカニズムでは文書が改ざんされたものとして検出してしまふ。しかし、このように文書の意味が変えられていない場合には、改ざんされていないものとして検出するような電子署名メカニズムが提供されれば、非常に有用性が高い。

【0021】次に、従来の電子署名のさらに他の問題点について述べる。改ざんをもくろむ者は、改ざんした文書のメッセージダイジェストが改ざん前のメッセージダイジェストに一致するように改ざんを工夫する。そのために印字不可能な文字が使われる。すなわち、文書を改ざんするとともに、この文書中に印字不可能な文字をいくつか挿入することで、改ざんした文書の内容を変えずに同じメッセージダイジェストを作ることが不可能とは言えない。

【0022】例えば、「費用は、10,000円です。」を「費用は100,000円です。」と改ざんしても、ダイジェストの不一致により改ざんが検出されるであろう。これに対して、「費用は、100,000円です。」あるいは「費用は、100,000円です。」のように、いくつかの空白文字を挿入していけば、もとのダイジェストと一致するものを探し出せる可能性がある。

【0023】しかしながら、従来は、電子署名の付加された文書の受信側において、上記のような改ざんの可能性あるいは文書の信頼性を示すような指標が全く与えられていなかった。

【0024】

【発明が解決しようとする課題】上述したように従来では、電子署名は文章全体に対して行われるため、文章全体から一部引用した部分に対しては、認証不能であるという問題点があった。また、従来では、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うようなことができなかった。

【0025】また、従来の電子署名では、文書を改ざんするとともに、この文書中に印字不可能な文字をいくつか挿入することで、もとの文書と同じメッセージダイジェストを作ることが不可能とは言えないが、この種の改ざんの可能性あるいは文書の信頼性を示すような指標が全く与えられていなかった。

【0026】本発明は、上記事情を考慮してなされたもので、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする電子署名付加方法及び電子署名装置を提供することを目的とする。

【0027】また、本発明は、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる電子署名付加方法及び電子署名装置を提供することを目的とする。

【0028】また、本発明は、印刷にも有効な電子署名付加方法及び電子署名装置を提供することを目的とする。また、本発明は、本文中の印字不可能な文字の挿入による電子署名の信頼性低下を防ぐアルゴリズムを提供することによって、改ざんの可能性を見積もり、受信者に注意を促すことの可能な電子署名検証方法を提供することを目的とする。

【0029】

【課題を解決するための手段】本発明（請求項1）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、電子化された文書を、該文書中に出現する予め定められた特定文字また

は特定文字列を区切りとして、複数の署名文に分割し、分割された署名文ごとに、該署名文をもとに署名情報を生成し、前記署名文に対応付けて前記署名情報を格納することを特徴とする。

【0030】本発明によれば、署名対象となる電子化文書を複数の署名文に分割し、署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名対の単位で引用することが可能となる。

【0031】本発明（請求項2）は、請求項1において、前記特定文字は、空白文字、句点文字、読点文字または括弧文字のうちの少なくとも1つであることを特徴とする。

【0032】本発明（請求項3）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名付加方法において、署名情報を付加する対象となる文書中から予め定められた特定文字を除外し、前記文書中から前記特定文字を除外して得られた文をもとに署名情報を生成し、前記署名情報を付加する対象となる文書に、生成された前記署名情報を付加することを特徴とする。

【0033】本発明によれば、特定文字を適宜設定することにより、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【0034】また、本発明において、除外対象とする特定文字を印字不可能な文字すべてとすれば、印字可能文字をもって文書を改ざんすることが事実上不可能になる。また、印字された後も電子署名による改ざん防止に役立つ。

【0035】本発明（請求項4）は、請求項3において、前記特定文字は、空白文字、句点文字、読点文字、括弧文字および印刷不可能な制御文字のうちの少なくとも1つであることを特徴とする。

【0036】本発明（請求項5）は、上記各発明において、前記署名情報は、該署名情報のもととなる文から所定のハッシュ関数を用いて生成したダイジェストを公開鍵暗号方式の所定の秘密鍵で暗号化したものであることを特徴とする。

【0037】本発明（請求項6）は、上記各発明において、前記署名情報は、該署名情報による署名対象となる文の前方または後方に挿入することを特徴とする。本発明（請求項7）に係る電子署名検証方法は、作者を証明する署名情報が付加された電子化された文書を受け取り、受け取った前記文書中の印字可能文字の総数と印字不可能文字の総数をもとに所定の計算式を用いて前記署名情報の信頼性を評価することを特徴とする。

【0038】本発明によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算

し、改ざんの可能性を評価することができる。そして、必要に応じて警告を発するなどして注意を促すことができる。

【0039】本発明（請求項8）は、請求項7において、前記特定文字は、印刷不可能な文字であることを特徴とする。本発明（請求項9）は、請求項7において、前記所定の計算式は、 p を印字不可能文字の種類、 m を文書の文字数、 k を印字不可能な文字の数、 l をメッセージダイジェストのビット長、信頼性の値を T としたとき、 $T = (p^k) \times (m+1) \times (m+2) \times \dots \times (m+k) / (2^l)$ で表されるものであり、求められた信頼性の値 T と予め定められたしきい値とを比較することにより前記署名情報の信頼性を評価することを特徴とする。

【0040】本発明（請求項10）は、電子化された文書に、該文書の作者を証明する署名情報を付加する電子署名装置において、電子化された文書を、該文書中出现する予め定められた特定文字または特定文字列を区切りとして、複数の署名文に分割する手段と、分割された署名文ごとに、該署名文をもとに署名情報を生成する手段と、前記署名文に対応付けて前記署名情報を格納する（前方または後方に挿入する）手段とを備えたことを特徴とする。

【0041】上記の方法に係る各発明は、装置に係る発明としても成立する。なお、以上の各発明について、相当する処理手順を実行させるプログラムを、コンピュータを制御するためのプログラムとしてコンピュータ読取可能な記憶媒体に格納し、コンピュータに該記憶媒体からプログラムを読取らせ、コンピュータ上で実行させることが可能である。

【0042】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。以下で説明する各実施形態の送信システムは、電子化文書を送信する送信側となる端末装置と、この電子化文書を受信する受信側となる端末装置と、これらをつなぐ媒体から構成される。もちろん、端末装置に送信機能及び受信機能の両方を設けても良い。媒体は、ネットワークであっても良いし、フロッピー・ディスクあるいはCD-ROMなど可搬性の情報記録媒体であっても良いし、少なくとも一部または全部に無線通信部分を含んでも良い。また、送信側となる端末装置から一旦、所定のサーバ装置等に蓄積され、その後、サーバ装置等から受信側となる端末装置に転送される形態でも良い。端末装置は、媒体に応じた送信装置、受信装置を持つものとする。

【0043】本実施形態において、署名文とは、署名対象となる一纏まりの文のことを言うものとする。また、処理後署名文とは、署名文から予め定められた文字を除外した文のことを言うものとする。第1の実施形態では、署名文からダイジェストを生成するのに対して、第

2の実施形態では、処理後署名文からダイジェストを生成する。なお、署名文も処理後署名文も平文である。

【0044】本実施形態において、データ本文とは、署名対象となる一纏まりの文書全文（平文）を言うものとする。また、署名つき文とは、電子署名の付加された署名文を連結したものを言うものとする。言い換えると、署名対象となるデータ本文に、署名文単位に生成された電子署名が付加あるいは挿入された文を言うものとする。

【0045】（第1の実施形態）第1の実施形態では、10 電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする発明の実施形態について説明する。

【0046】まず、本実施形態の電子署名付加装置（電子署名装置）について説明する。図1は、本電子署名付加装置の構成を示す図である。また、図2は、本電子署名付加装置による署名付加処理の手順を示すフローチャートである。

【0047】電子署名付加装置は、送信側の端末装置内に設けられる。図1に示すように、電子署名付加装置 20 は、区切り文字検出部2、ダイジェスト生成部4、暗号化部8、秘密鍵記憶部10、署名つき文生成部12を備えている。

【0048】図1中のデータ本文は、署名を付加する本文全体であり、複数の文章や段落などから構成されている通常の文書である。区切り文字検出部2は、データ本文から予め定められた位置または複数の区切り文字を検出し、データ本文を、該区切り文字を末尾とする適当な長さの署名文に区切って行く（ステップS11）。

【0049】検出する区切り文字としては、任意の位置 30 または複数のものを定義することができる。例えば、検出する区切り文字として、ピリオド“.”および読点“。”を用いる。もちろん、ピリオド“.”および読点“。”の一方だけ定めても有効な場合もある。あるいは、文末文字“ASCII:nl=0A(hex)”

”および段落末文字“ASCII:cr=0D(hex)”の一方だけを用いる方法もある。また、上記ピリオド“.”および読点“。”の少なくとも一方に、さらに句点“、”、閉じる括弧“]”、“}”、“)”や文末文字“ASCII:nl=0A(hex)”や段落末文字“ASCII:cr=0D(hex)”の少なくとも一つを加えて、適宜定義することができる。もちろん、この他にも種々の区切り文字の定義が可能である。

【0050】図3に、本区切り文字検出部2の処理手順の一例を示す。予め区切り文字を定め（例えば句点“、”と読点“。”とする）、これを区切り文字リスト14に登録しておく。まず、データ本文中から一文字入力しバッファ（図示せず）に入れる（ステップS21）。ここで、バッファに入力した文字が区切り文字リ 50

スト14に登録された文字であるか否かを判定し（ステップS22）、区切り文字でなかった場合、データ本文中から次の一文字を入力しバッファに入れる。

【0051】上記の処理を繰り返し、ステップS22でバッファに入れた文字が区切り文字であった場合（例えば句点“、”または読点“。”であった場合）に、バッファを出て（ステップS23）、1つの署名文（例えば句点“、”または読点“。”を末尾とするもの）が得られる。

【0052】ダイジェスト生成部4は、既に説明したようなハッシュ関数6によって署名文から、ダイジェストを生成する（ステップS12）。用いるハッシュ関数、ダイジェストのビット長は、予め決めておくものとする。本実施形態では、ハッシュ関数6として「MD5」を用い、ダイジェストのビット長は128ビットとする。ハッシュ関数としてSHAを用いる場合は、ダイジェストのビット長は160ビットとなる。また、ハッシュアルゴリズムとして他のものを用いても構わない。なお、用いるハッシュ関数を選択可能として、実際に用いたハッシュ関数（あるいはハッシュ関数とダイジェストのビット長）を示す情報を署名つき文に付加することも可能である。

【0053】暗号化部8は、秘密鍵記憶部10に記憶されている公開鍵暗号方式の秘密鍵を用いてダイジェストを暗号化する（ステップS13）。この暗号化されたダイジェストが電子署名として用いられる。ここでは、公開鍵暗号方式としてRSA方式を用いることとする。

【0054】ここで、セキュリティ上、上記秘密鍵は他人に知得されないようにするのが好ましい。例えば、上記秘密鍵記憶部10としてICカードを用い、ICカードに上記秘密鍵を記録しておき、必要時に、例えば本署名付加処理を行うときに、該ICカードをICカード・リーダー（図示しない）にセットし、ICカード・リーダーから読み取った秘密鍵を暗号部8に渡すようにする。

【0055】署名つき文生成部12は、区切り文字検出部2にて得られた署名文夫々に対して電子署名を付加して行く（ステップS14）。ここでは、署名文の後に電子署名を挿入して署名つき文を生成するものとする。なお、署名文の前に電子署名を挿入しても良いし、電子署名をまとめて全文書の前にヘッダとして挿入しても良い。

【0056】そして、ステップS15で、現在の署名文がデータ本文の最後の文章かどうかを判定する。最後でなければ再び区切りステップS11の文字列検出部2による処理に戻り、ステップS15でデータ本文が終りとなるまでステップS11～ステップS14の処理を繰り返す。

【0057】この結果、例えば図4に示すような署名つき文を得ることができる。ここでは、署名文（分割メッ

セージ)の後に電子署名を挿入した結果、データ本文中の適当な間隔に署名が挿入された形になっている。

【0058】なお、電子署名中には、それが電子署名のデータであることが判るような情報を含ませることが望ましい。例えば、電子署名本体(ダイジェストを暗号化したデータ)を“##Signature=”と“##”で挟んだデータを用いることができる。

【0059】また、各署名文には、先頭のもののからの序列を示すシーケンス番号(およびシーケンス番号であることを示す所定の情報;例えば##SN=”と“##”でシーケンス番号を挟む)を付加しても良い(例えば各署名文の直前)。このようにすると、受信側での処理(例えば署名文の分割処理)が容易となる。また、上記のように電子署名をまとめて全文書の前にヘッダとして挿入する場合、ヘッダ内でシーケンス番号を用いて署名文と電子署名との対応を取ることができる。

【0060】次に、本実施形態の電子署名検証装置について説明する。図5は、本実施形態の電子署名検証装置の構成を示す図である。また、図6は、本電子署名検証装置による署名検証処理の手順を示すフローチャートである。

【0061】電子署名検証装置は、受信側の端末装置内に設けられる。図5に示すように、電子署名検証装置は、署名分割部22、ダイジェスト生成部24、復号部28、公開鍵記憶部30、比較部32を備えている。

【0062】図5中の署名つき文は、所定の媒体を通じて受け取った電子化文書であり、前述の電子署名付加装置によって電子署名が付加された文書である。電子署名は例えば図4のように文書中の適当な位置に挿入されている。

【0063】署名分割部22は、署名つき文から、1組の署名文と電子署名を取り出す(ステップS31)。これには幾つかの方法が考えられる。1つは、電子署名が付加されたときに区切り文字検出部2により用いられたものと同一の処理を用いて署名文を取り出すとともに、署名文の前あるいは後などの決められた位置に付加されている所定ビット長の電子署名を取り出す方法である。他の1つは、例えば前述のように電子署名の一部に“##Signature=”と“##”からなるラベルを付加した場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。さらに他の方法は、各署名文に##SN=”と“##”からなるラベルで挟まれたシーケンス番号が付加されている場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。

【0064】次に、復号部28は、公開鍵記憶部30に記憶されている公開鍵暗号方式の公開鍵を用いて電子署名を復号するして、ダイジェスト(ダイジェスト#1とする)に戻す(ステップS32)。

【0065】ここで、公開鍵は、電子署名が付加された

ときに暗号化部8により用いられた秘密鍵に対応するものを用いる。例えば、暗号化の際に公開鍵暗号方式(RSA)の秘密鍵が用いられた場合、該秘密鍵に一意に対応する公開鍵暗号方式(RSA)の公開鍵を用いる。この公開鍵は、例えば署名つき文に付加された情報(例えば本文書の作成者の持つユーザIDあるいは送信元アドレスなど)をたよりに公開鍵サーバあるいは公開鍵データベースなどから入手できるものとする。

【0066】一方、ダイジェスト生成部24は、電子署名が付加されたときにダイジェスト生成部4により用いられたものと同一のハッシュ関数によって、取り出した署名文に対するダイジェスト(ダイジェスト#2とする)を生成する(ステップS33)。

【0067】ここで、復号部28によるダイジェスト#1の生成処理と、ダイジェスト生成部24によるダイジェスト#2の生成処理とは、いずれを先に行っても良いし、並列実行しても良い。

【0068】比較部32は、ダイジェスト#1とダイジェスト#2の比較を行う(ステップS34)。もし両者が一致すれば、その署名文は改ざんされていないので、その署名文に対する認証結果情報を、有効を示す情報(例えば1)とする(ステップS35)。もし両者が不一致ならば、その署名文の改ざんを検出したことになるので、その署名文に対する認証結果情報を、無効を示す情報(例えば0)とする(ステップS35)。認証結果情報は、例えば、該当する電子署名の直後にまたは直前に付加する方法、あるいは各署名文に##SN=”と“##”からなるラベルで挟まれたシーケンス番号が付加されている場合、シーケンス番号と認証結果情報との対を記録して行く方法などが考えられる。

【0069】以上の処理を、ステップS37で文書の終りが検出されるまで、繰り返し行う。図7は、本電子署名検証装置による他の署名検証処理の手順を示すフローチャートである。本手順は、1つでも改ざんの検出された署名文が存在する場合、文書全体を無効とするようにした例である。

【0070】この場合、ステップS31～ステップS34の比較と、ステップS37での文書の終りの検出は、図6と同様であるが、図7の手順ではステップS34の比較において一致がみられた場合、何も記録せず、ステップS34の比較において不一致がみられた場合、その時点で異常終了とし、ステップS37での文書の終りが検出され、全署名文について改ざんが検出されなかった場合に、正常終了とする。

【0071】なお、各端末に、電子署名付加装置と電子署名検証装置の機能を持たせることが可能である。この場合、ダイジェスト生成部やハッシュ関数など構成部分の共通化を行うことができる。

【0072】以上のように本実施形態によれば、データ本文に対し署名文単位に電子署名を付加するので、電子

化文書から署名文・電子署名の対の単位で抜き出して引用することが可能となる。

【0073】(第2の実施形態)第2の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とするのに加え、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした発明の実施形態について説明する。

【0074】まず、本実施形態の電子署名付加装置について説明する。図8は、本電子署名付加装置(電子署名装置)の構成を示す図である。また、図9は、本電子署名付加装置による署名付加処理の手順を示すフローチャートである。

【0075】電子署名付加装置は、送信側の端末装置内に設けられる。図8に示すように、電子署名付加装置は、区切り文字検出部102、ダイジェスト生成部104、暗号化部108、秘密鍵記憶部110、署名つき文生成部112を備えている。

【0076】図8中のデータ本文は、署名を付加する本文全体であり、複数の文章や段落などから構成されている通常の文書である。区切り文字検出部102は、データ本文から予め定められた位置または複数の区切り文字を検出し、データ本文を、該区切り文字を末尾とする適当な長さの署名文に区切って行くとともに、印字不可能文字除外部103を用いて予め定められた印字不可能文字を署名文から除外した処理後署名文を生成する(ステップS111)。

【0077】検出する区切り文字としては、任意の位置または複数のものを定義することができる。例えば、検出する区切り文字として、ピリオド“.”および読点“。”を用いる。もちろん、ピリオド“.”および読点“。”の一方だけ定めても有効な場合もある。あるいは、文末文字“ASCII:n1=0A(hex)”

”および段落末文字“ASCII:cr=0D(hex)”の一方だけを用いる方法もある。また、上記ピリオド“.”および読点“。”の少なくとも一方に、さらに句点“、”、閉じる括弧“]”、

“}”、“)”や文末文字“ASCII:n1=0A(hex)”や段落末文字“ASCII:cr=0D(hex)”の少なくとも一つを加えて、適宜定義することができる。もちろん、この他にも種々の区切り文字の定義が可能である。

【0078】区切り文字検出部102により署名文を生成する処理手順の一例は図3と同様である。すなわち、予め区切り文字を定め、これを区切り文字リスト114に登録しておく。まず、データ本文中から一文字入力しバッファ(図示せず)に入れる(ステップS21)。ここで、バッファに入力した文字が区切り文字リスト11

4に登録された文字であるか否かを判定し(ステップS22)、区切り文字でなかった場合、データ本文中から次の一文字を入力しバッファに入れる。

【0079】次に、区切り文字検出部102により文書の区切り検出と署名に加味しない文字の排除を行って処理後署名文を生成する処理手順の一例について説明する。図10は、区切り文字検出部102により処理後署名文を生成する処理手順の一例を示す。

【0080】署名対象となるデータ本文から、まず、一文字の入力文字を取り出し(ステップS121)、印字不可能リスト113を参照して、その文字が予め定められた印字不可能文字か否かを検出する(ステップS122)。

【0081】ここで、印字可能な文字は、少なくとも何らかの印字が行われる文字であり、a, b, c, ..., 1, 2, 3, ..., あ, い, う, ..., 吾, 亜, 阿, ..., などである。一方、印字不可能な文字は、空白、タブ、改行など、何の印字もされない文字である。例えば、後者の文字をASCIIコード表で表すと図11中で太線で囲った範囲のものとなる。

【0082】印字不可能な文字をすべて印字不可能リスト113に登録しておく。この印字不可能リスト113を参照することによって署名に加味しない文字が除外される。なお、除外対象とする印字不可能な文字を予め定めた一部のものとし、それらを印字不可能リスト113に登録しておくことも可能である。例えば、改行文字は除外しないようにすることができる。

【0083】次に、文字リスト114を参照して、文字の区切りであるか否かが検出される(ステップS123)。なお、区切り文字として採用した文字は、このアルゴリズムを用いる場合には、印字不可能リスト113から除外する。もしステップS123の区切り検出をステップS112の印字可能検出より前に行う場合は、印字不可能リスト113の中に区切り文字が含まれていても構わない。

【0084】さて、ステップS123で区切り文字でなかった場合、その文字はバッファ(図示せず)に蓄えられ(ステップS124)、ステップS121に戻って、次の一文字が取り出され、同様の処理が繰り返される。

【0085】一方、ステップS123で区切り文字であった場合は、処理後署名文が形成されたことになるので、バッファをフラッシュして、以後の処理に署名文書を引き渡す(ステップS125)。このようにして、本文中から処理後署名文を取り出すことができる。

【0086】なお、区切り文字検出部102による署名文の生成と処理後署名文の生成は、どのような順序で行っても良いし、同時に行っても良い。また、まず、署名文を生成し、生成された署名文から予め定められた印字不可能文字を除外することによって処理後署名文を生成しても良い。また、例えば、図3のフローチャートと図

10のフローチャートをもとに、署名文と処理後署名文を同時に生成するフローチャートを作り出すことも容易である（この場合、署名文用と処理後署名文用の2つのバッファを用いる）。

【0087】なお、上記では、区切り文字検出部102は、区切り文字を検出しているが、その代わりに、区切り文字列を検出するようにしても良い。例えば、読点“。”や改行文字が単独で現れただけでは文の区切りとせず、読点“。”と改行文字が続けて現れた場合に文の区切りとする。

【0088】次に、ダイジェスト生成部104は、既に説明したようなハッシュ関数106によって処理後署名文からダイジェストを生成する（ステップS112）。用いるハッシュ関数、ダイジェストのビット長は、予め決めておくものとする。本実施形態では、ハッシュ関数106として「MD5」を用い、ダイジェストのビット長は128ビットとする。ハッシュ関数としてSHAを用いる場合は、ダイジェストのビット長は160ビットとなる。また、ハッシュアルゴリズムとして他のものを用いても構わない。なお、用いるハッシュ関数を選択可能として、実際に用いたハッシュ関数（あるいはハッシュ関数とダイジェストのビット長）を示す情報を署名つき文に付加することも可能である。

【0089】暗号化部108は、秘密鍵記憶部110に記憶されている公開鍵暗号方式の秘密鍵を用いてダイジェストを暗号化する（ステップS113）。この暗号化されたダイジェストが電子署名として用いられる。ここでは、公開鍵暗号方式としてRSA方式を用いることとする。

【0090】ここで、セキュリティ上、上記秘密鍵は他人に知得されないようにするのが好ましい。例えば、上記秘密鍵記憶部110としてICカードを用い、ICカードに上記秘密鍵を記録しておき、必要時に、例えば本署名付加処理を行うときに、該ICカードをICカード・リーダー（図示しない）にセットし、ICカード・リーダーから読み取った秘密鍵を暗号部108に渡すようにすることができる。

【0091】署名つき文生成部112は、区切り文字検出部102にて得られた署名文夫々に対して電子署名を付加して行く（ステップS114）。ここでは、署名文の後に電子署名を挿入して署名つき文を生成するものとする。なお、署名文の前に電子署名を挿入しても良いし、電子署名をまとめて全文書の前にヘッダとして挿入しても良い。

【0092】そして、ステップS115で、現在の署名文がデータ本文の最後の文章かどうかを判定する。最後でなければ再び区切りステップS111の文字列検出装置102による処理に戻り、ステップS115でデータ本文が終りとなるまでステップS111～ステップS114の処理を繰り返す。

【0093】この結果、例えば図3に示すような署名つき文を得ることができる。ここでは、署名文の後に電子署名を挿入する結果、データ本文中の適当な間隔に署名が挿入された形になっている。

【0094】なお、電子署名には、それが署名文のデータではなく電子署名のデータであることが判るような情報を含ませることが望ましい。例えば、電子署名本体を“##Signature=”と“##”で挟んだデータを用いることができる。

10 【0095】また、各署名文には、先頭のもののからの序列を示すシーケンス番号（およびシーケンス番号であることを示す所定の情報；例えば##SN=”と“##”でシーケンス番号を挟む）を付加しても良い（例えば各署名文の直前）。このようにすると、受信側での処理（例えば署名文の分割処理）が容易となる。また、上記のように電子署名をまとめて全文書の前にヘッダとして挿入する場合、ヘッダ内でシーケンス番号を用いて署名文と電子署名との対応を取ることができる。

20 【0096】次に、本実施形態の電子署名検証装置について説明する。図12は、本実施形態の電子署名検証装置の構成を示す図である。また、図13は、本電子署名検証装置による署名検証処理の手順を示すフローチャートである。

【0097】電子署名検証装置は、受信側の端末装置内に設けられる。図13に示すように、電子署名検証装置は、署名分割部122、印字不可能文字除外部123、ダイジェスト生成部124、復号部128、公開鍵記憶部130、比較部132を備えている。

【0098】図12中の署名つき文は、所定の媒体を通じて受け取った電子化文書であり、前述の電子署名付加装置によって電子署名が付加された文書である。電子署名は例えば図4のように文書中の適当な位置に挿入されている。

【0099】署名分割部122は、署名つき文から、1組の署名文と電子署名を取り出す（ステップS131）。これには幾つかの方法が考えられる。1つは、電子署名が付加されたときに区切り文字検出部2により用いられたものと同一の処理を用いて署名文を取り出すとともに、署名文の前あるいは後などの決められた位置に付加されている所定ビット長の電子署名を取り出す方法である。他の1つは、例えば前述のように電子署名の一部に“##Signature=”と“##”からなるラベルを付加した場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。さらに他の方法は、各署名文に##SN=”と“##”からなるラベルで挟まれたシーケンス番号が付加されている場合、このラベルを検出して行くことで、容易に各組の署名文と電子署名を取り出すことができる。

50 【0100】次に、復号部128は、公開鍵記憶部13

0に記憶されている公開鍵暗号方式の公開鍵を用いて電子署名を復号するして、ダイジェスト（ダイジェスト#1とする）に戻す（ステップS132）。その際、公開鍵は、電子署名が付加されたときに暗号化部108により用いられた秘密鍵に対応するものを用いる。例えば、暗号化の際に公開鍵暗号方式（RSA）の秘密鍵が用いられた場合、該秘密鍵に一意に対応する公開鍵暗号方式（RSA）の公開鍵を用いる。この公開鍵は、前述したように、例えば署名つき文に付加された情報をたよりに入手できるものとする。

【0101】一方、印字不可能文字除去部123は、電子署名が付加されたときに印字不可能文字除外部103により用いられたものと同一の印字不可能リスト113を用いて、署名文から予め定められた印字不可能文字を除外して、処理後署名文を生成する（ステップS133-1）。

【0102】そして、ダイジェスト生成部124は、電子署名が付加されたときにダイジェスト生成部104により用いられたものと同一のハッシュ関数によって、生成された処理後署名文に対するダイジェスト（ダイジェスト#2とする）を生成する（ステップS133-2）。

【0103】ここで、復号部128によるダイジェスト#1の生成処理と、印字不可能文字除去部123およびダイジェスト生成部124によるダイジェスト#2の生成処理とは、いずれを先に行っても良いし、並列実行しても良い。

【0104】比較部132は、ダイジェスト#1とダイジェスト#2の比較を行う（ステップS134）。もし両者が一致すれば、その署名文は改ざんされていないので、その署名文に対する認証結果情報を、有効を示す情報（例えば1）とする（ステップS135）。もし両者が不一致ならば、その署名文の改ざんを検出したことになるので、その署名文に対する認証結果情報を、無効を示す情報（例えば0）とする（ステップS135）。認証結果情報は、例えば、該当する電子署名の直後にまたは直前に付加する方法、あるいは各署名文に##SN＝”と”##”からなるラベルで挟まれたシーケンス番号が付加されている場合、シーケンス番号と認証結果情報との対を記録して行く方法などが考えられる。

【0105】以上の処理を、ステップS137で文書の終りが検出されるまで、繰り返し行う。図14は、本電子署名検証装置による他の署名検証処理の手順を示すフローチャートである。本手順は、1つでも改ざんの検出された署名文が存在する場合、文書全体を無効とするようにした例である。

【0106】ステップS131～ステップS134の比較と、ステップS137での文書の終りの検出は、図13と同様であるが、図14の手順ではステップS134の比較において一致がみられた場合、何も記録せず、ス

テップS134の比較において不一致がみられた場合、その時点で異常終了とし、ステップS137での文書の終りが検出され、全署名文について改ざんが検出されなかった場合に、正常終了とする。

【0107】なお、各端末に、電子署名付加装置と電子署名検証装置の機能を持たせることが可能である。この場合、ダイジェスト生成部やハッシュ関数など構成部分の共通化を行うことができる。

【0108】以上のように本実施形態によれば、データ本文に対し署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名の対の単位で抜き出して引用することが可能となる。また、印字された後も電子署名による改ざん防止に役立つ。

【0109】また、本発明は、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【0110】また、本実施形態において、印字不可能な文字をすべて除外対象とすれば、改ざんした文書に印字不可能文字を挿入してもと同じダイジェストを作成することが不可能になる。

【0111】さて、第1の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とする発明の実施形態について説明し、第2の実施形態では、電子署名された電子化文書中から一部を引用しても、該引用した一部の文についての認証を可能とするのに加え、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした発明の実施形態について説明したが、他の実施形態として、データ本文を署名文単位に分割せず、電子署名をデータ本文全体に対して付加するものであって、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができるようにした実施形態も可能である。

【0112】この場合の実施形態は、例えば、第2に実施形態において、区切り文字を検出して署名文を生成する構成部分、すなわちデータ本文を署名文単位に分割する構成部分を削除することで容易に構成可能である。すなわち、電子署名付加装置側では、データ本文から予め定められた印字不可能文字を削除して、ダイジェストを生成し、これを暗号化し、これによって得られた電子署名を該データ本文に付加すれば良い。一方、電子署名検証装置側では、受け取ったデータ本文から予め定められた印字不可能文字を削除して、ダイジェスト#1を生成するとともに、データ本文に付加された電子署名を復号

してダイジェスト#2を生成し、ダイジェスト#1とダイジェスト#2を比較すれば良い。

【0113】(第3の実施形態)第3の実施形態では、改ざんした文書に空白などの印字不可能文字を挿入してもと同じダイジェストが作成された可能性についての指標を与えるようにした発明の実施形態について説明する。

【0114】従来例で説明したように、改ざんをもくろむ者は、改ざんした文書のメッセージダイジェストが改ざん前のメッセージダイジェストに一致するように改ざんを工夫する。そのために印字不可能な文字が使われる。

【0115】まず、文書の文字数を m とする。この中に印字不可能な文字を一つ挿入することで、文書の内容自体を変えずに同じメッセージダイジェストを作ることができる可能性がある。不正に作られるダイジェストの数は、挿入する印字不可能な文字の種類 p とこれを挿入する位置 $(m+1)$ の積により次式のように表される。

$$L = p \times (m+1)$$

L_1 = (一つの印字不可能文字の付加によって作られるダイジェストの数)

p = (印字不可能文字の種類)

m = (文書の文字数)

2個の印字不可能文字を付加する場合、2個の組み合わせは p の2乗通りあり、またその位置は1個目に可能な挿入位置 $(m+1)$ と2個目に可能な挿入位置の数 $(m+2)$ との積で近似できる。したがって、 k 個の印字不可能文字が付加されている場合、不正に作ることができるダイジェストの数 L_k は、次式のように表される。

$$L_k = (p^k) \times (m+1) \times (m+2) \times \dots \times (m+k)$$

L_k = (k 個の印字不可能文字の付加によって作られるダイジェストの数)

p = (印字不可能文字の種類)

m = (文書の文字数)

k = (印字不可能な文字の数)

一方、メッセージダイジェストのビット長を1とすると、正当な手段で作出されるメッセージダイジェストの数は 2^1 である。したがって、これに対する不正に作られるメッセージダイジェストの数 L_k の割合が、メッセージダイジェストの信頼性の指数となる。

$$T = (p^k) \times (m+1) \times (m+2) \times \dots \times (m+k) / (2^1)$$

p = (印字不可能文字の種類)

m = (文書の文字数)

k = (印字不可能な文字の数)

1 = (メッセージダイジェストのビット長)

図15は、 $T=0.0001$ 、すなわち1万分の1以下の確率で改ざんが可能になると考えられる印字不可能な文字の最大数を、文書の文字数(有効文字数)とダイジ

ェストのビット長をパラメータに計算した結果である。ここで、印字不可能な文字の種類は34とした。

【0116】これによれば、 1000 (nearly equal 2^{10}) 文字の文書に対して128ビットのメッセージダイジェストを作った場合、印字不可能な文字が7文字以下ならばダイジェストの信頼度は十分(改ざん可能な確率は1万分の1以下)であることが判る。もちろん文書の種類によってはそれ以上の信頼度を必要とする場合がある。しかし、同様の計算を行うことで所望の信頼度を確保することが可能となる。この計算に用いたC言語によるプログラムを図16に示す。

【0117】図17は、本実施形態の信頼性評価装置の構成を示す図である。また、図18は、本信頼性評価装置による信頼性評価処理の手順を示すフローチャートである。

【0118】信頼性評価装置は、受信側の端末装置内に設けられる。図17に示すように、信頼性評価装置は、文字数計数部201、信頼性計算部202、評価部203を備えている。

【0119】まず、文字数計数部201により、1つの署名文から1文字ずつ取り出され(ステップS201)、印字可能かどうか判定される(ステップS202)。印字可能ならば m に1を加え(ステップS204)、印字不可能ならば k に1が加えられる(ステップS203)。ステップS201、ステップS202とステップS203またはステップS204の処理を、ステップS205で1つの署名文が終わるまで繰り返すことにより、印字可能な文字の数 m と印字不可能な文字の数 k を数え上げる。

【0120】次に、信頼性計算部202は、例えば図16で示したプログラムにより信頼性を計算する(ステップS206)。そして、評価部203では、求められた信頼性の値が一定のしきい値(ここでは0.0001)以下であるかを判定する(ステップS207)。信頼性の値がしきい値より大きければ改ざんされた可能性がある旨のメッセージを表示装置(図示せず)に表示するなどして警告を発する(ステップS208)。

【0121】この信頼性評価処理の後に、所定の電子署名検証処理(例えば図21の従来の電子署名検証あるいは第1の実施形態の電子署名検証など)が行われる(ステップS209)。

【0122】以上のように本実施形態によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算し、改ざんの可能性を評価することができる。そして、必要に応じて警告を発するなどして注意を促すことができる。

【0123】なお、以上の各実施形態における各装置は、ハードウェアで構成することもできるが、各処理を行う部分をソフトウェアで構成することもできる。また、例えば、相当する処理手順を実行させるプログラム

を、コンピュータを制御するためのプログラムとしてコンピュータ読取可能な記憶媒体に格納し、コンピュータに該記憶媒体からプログラムを読取らせ、コンピュータ上で実行させることが可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0124】

【発明の効果】本発明によれば、署名対象となる電子化文書を複数の署名文に分割し、署名文単位に電子署名を付加するので、電子化文書から署名文・電子署名対の単位で引用することが可能となる。

【0125】また、本発明によれば、署名情報を付加する対象となる文書中から予め定められた特定文字を除外して署名情報を生成するので、特定文字を適宜設定することにより、電子署名された文書中に空白や改行といった文書の意味に関与しない制御文字を挿入したような場合、すなわち文書の意味自体は変えられていない場合には、文書が改ざんされていないものとして扱うことができる。

【0126】また、本発明によれば、印字された後も電子署名による改ざん防止に役立つ。また、本発明によれば、印字可能文字の総数と印字不可能文字の総数をもとに電子署名の信頼性を計算し、改ざんの可能性を評価することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る電子署名付加装置の構成を示す図

【図2】同実施形態の署名付加処理の手順を示すフローチャート

【図3】区切り文字検出部による署名文生成処理手順の一例を示すフローチャート

【図4】署名つき文の一例を示す図

【図5】同実施形態の電子署名検証装置の構成を示す図

【図6】同実施形態の署名検証処理の手順を示すフローチャート

【図7】同実施形態の他の署名検証処理の手順を示すフローチャート

【図8】本発明の第2の実施形態に係る電子署名付加装置の構成を示す図

【図9】同実施形態の署名付加処理の手順を示すフローチャート

【図10】区切り文字検出部による処理後署名文生成処*

* 理手順の一例を示すフローチャート

【図11】ASCIIコードにおける印字不可能文字を示す図

【図12】同実施形態の電子署名検証装置の構成を示す図

【図13】同実施形態の署名検証処理の手順を示すフローチャート

【図14】同実施形態の他の署名検証処理の手順を示すフローチャート

【図15】1万分の1以下の確率で改ざんが可能になると考えられる印字不可能な文字の最大数を、文書の文字数（有効文字数）とダイジェストのビット長をパラメータに計算した結果を示す図

【図16】署名信頼度計算プログラムの一例を示す図

【図17】本発明の第3の実施形態に係る信頼性評価装置の構成を示す図

【図18】同実施形態の信頼性評価処理の手順を示すフローチャート

【図19】従来の電子署名の仕組みを説明するための概念図

【図20】従来の電子署名付加方法を説明するための流れ図

【図21】従来の電子署名検証方法を説明するための流れ図

【図22】従来の電子署名における文章の部分引用を説明するための図

【符号の説明】

2, 102…区切り文字検出部

4, 24, 104, 124…ダイジェスト生成部4

6, 26, 106, 126…ハッシュ関数6

8, 108…暗号化部

10, 110…秘密鍵記憶部

12, 112…署名つき文生成部

22, 122…署名分割部

28, 128…復号部

30, 130…公開鍵記憶部

132, 32…比較部

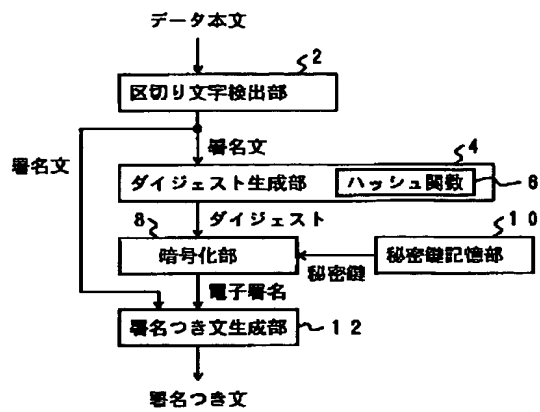
103, 123…印字不可能文字除外部

201…文字数計数部

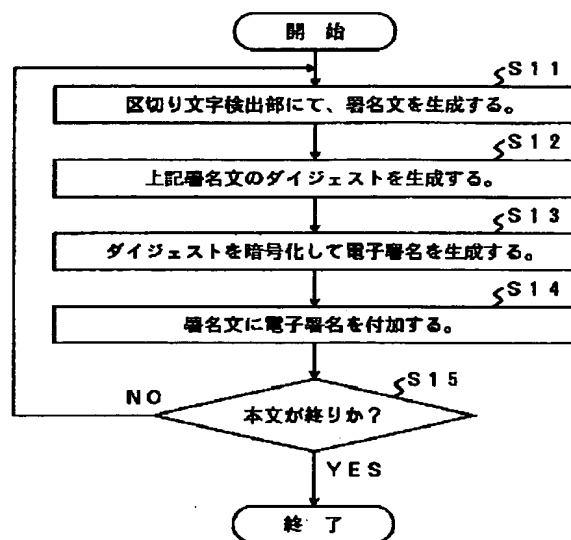
202…信頼性計算部

203…評価部

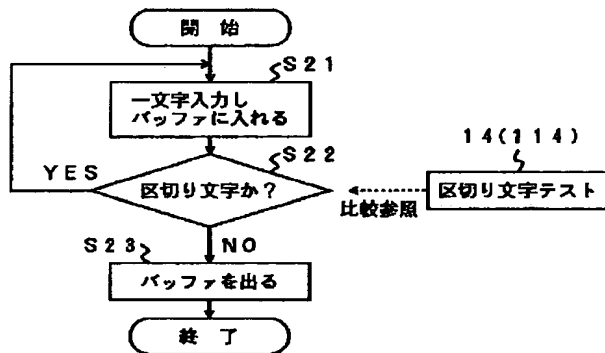
【図1】



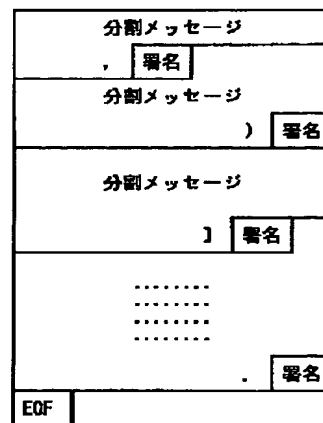
【図2】



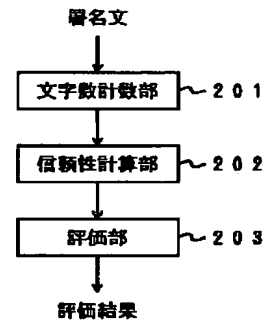
【図3】



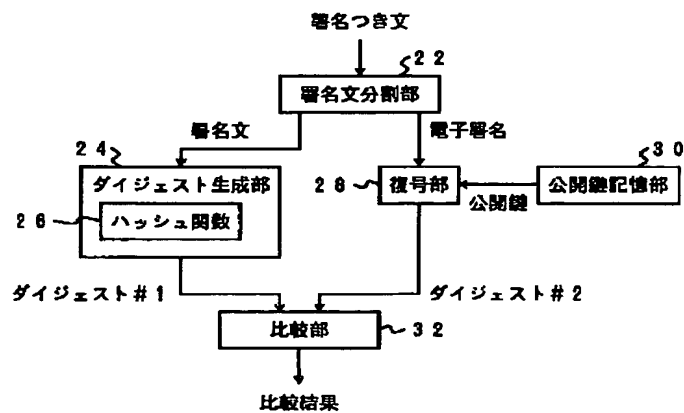
【図4】



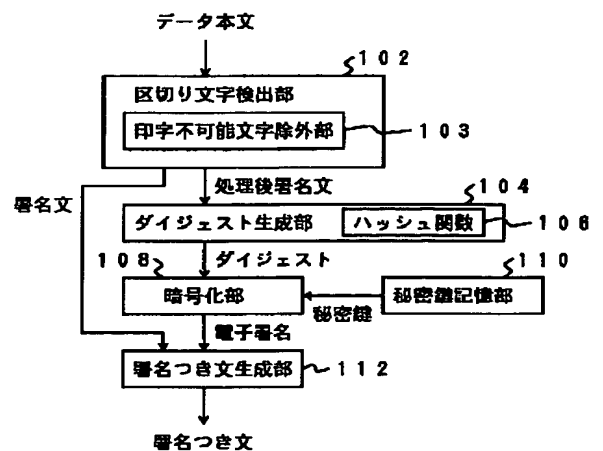
【図17】



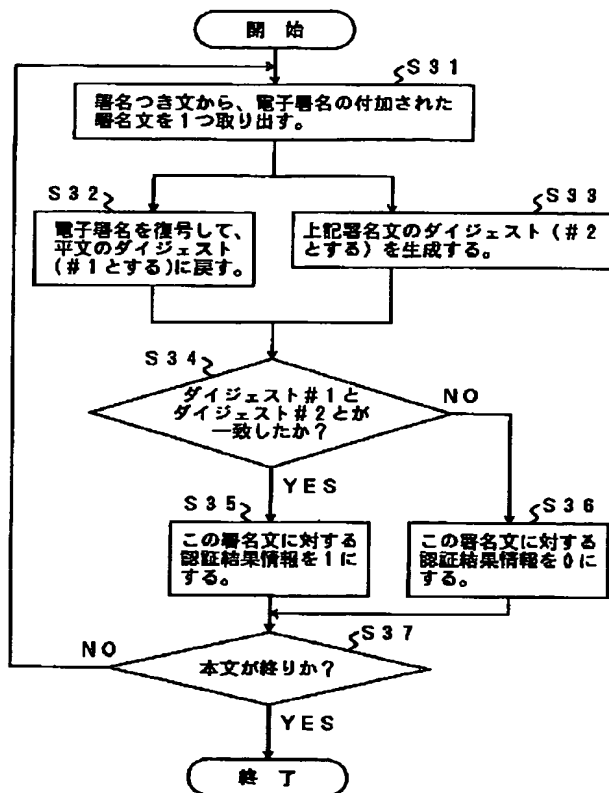
【図5】



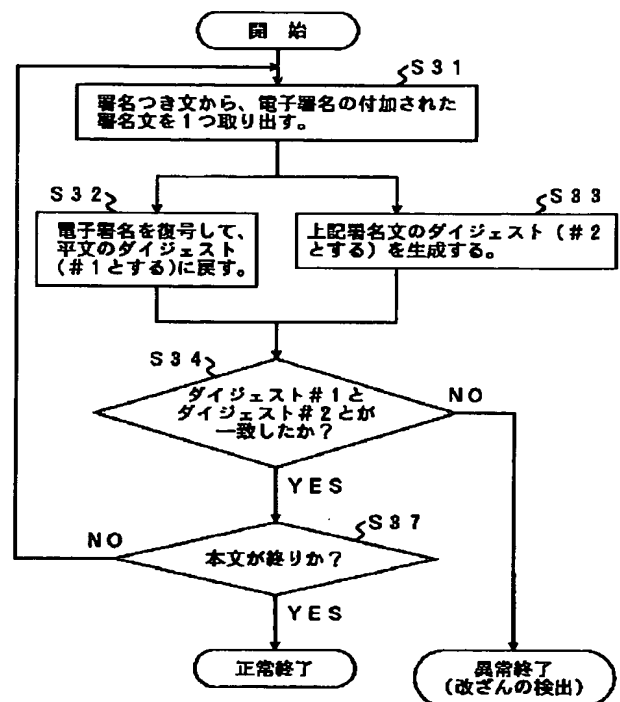
【図8】



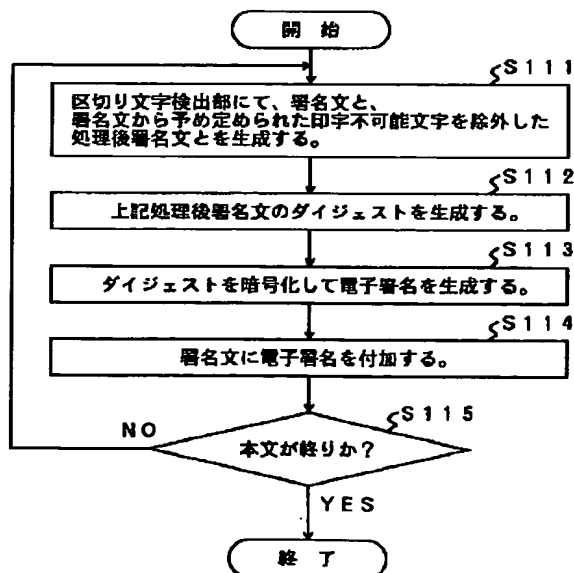
【図6】



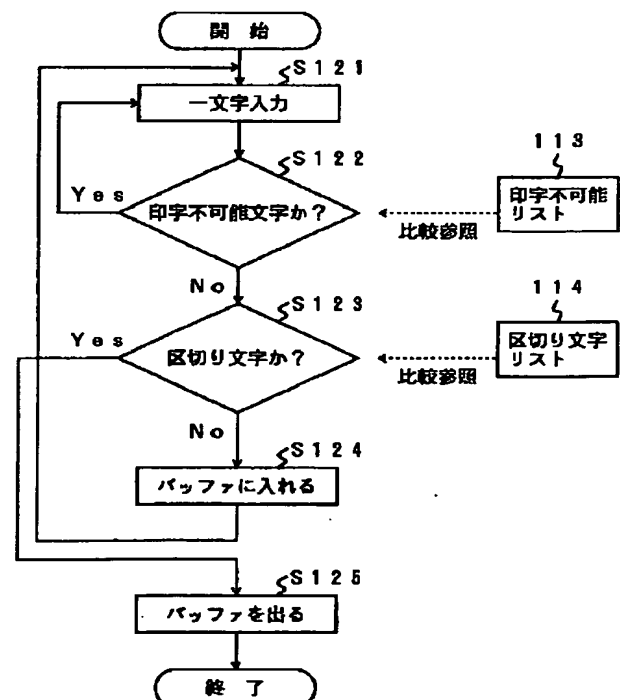
【図7】



【図9】



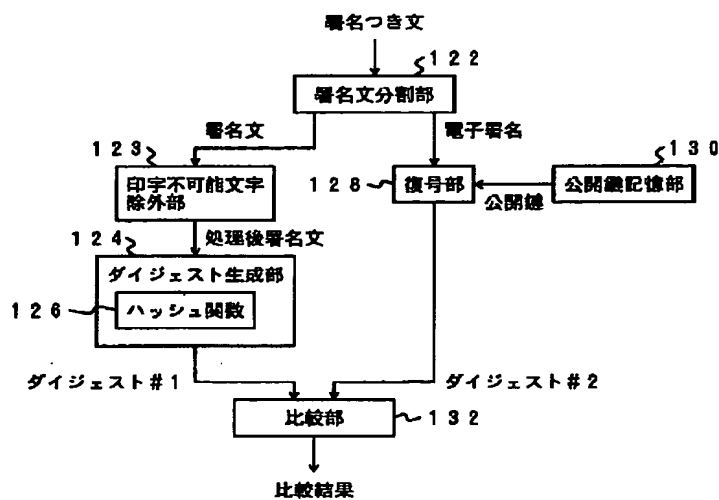
【図10】



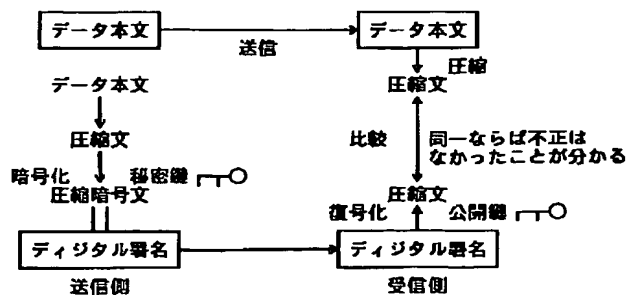
【図11】

000 nul	001 soh	002 stx	003 etx	004 eot	005 enq	006 ack	007 bel
010 bs	011 ht	012 nl	013 vt	014 np	015 cr	016 so	017 si
020 dle	021 dc1	022 dc2	023 dc3	024 dc4	025 nak	026 syn	027 etb
030 can	031 em	032 sub	033 esc	034 fs	035 gs	036 rs	037 us
040 sp	041 !	042 "	043 #	044 \$	045 %	046 &	047 '
050 (051)	052 *	053 +	054 ,	055 -	056 _	057 /
060 0	061 1	062 2	063 3	064 4	065 5	066 6	067 7
070 8	071 9	072 :	073 ;	074 <	075 =	076 >	077 ?
100 @	101 A	102 B	103 C	104 D	105 E	106 F	107 G
110 H	111 I	112 J	113 K	114 L	115 M	116 N	117 O
120 P	121 Q	122 R	123 S	124 T	125 U	126 V	127 W
130 X	131 Y	132 Z	133 [134 \	135]	136 ^	137 _
140 `	141 a	142 b	143 c	144 d	145 e	146 f	147 g
150 h	151 i	152 j	153 k	154 l	155 m	156 n	157 o
160 p	161 q	162 r	163 s	164 t	165 u	166 v	167 w
170 x	171 y	172 z	173 {	174	175 }	176 ~	177 del

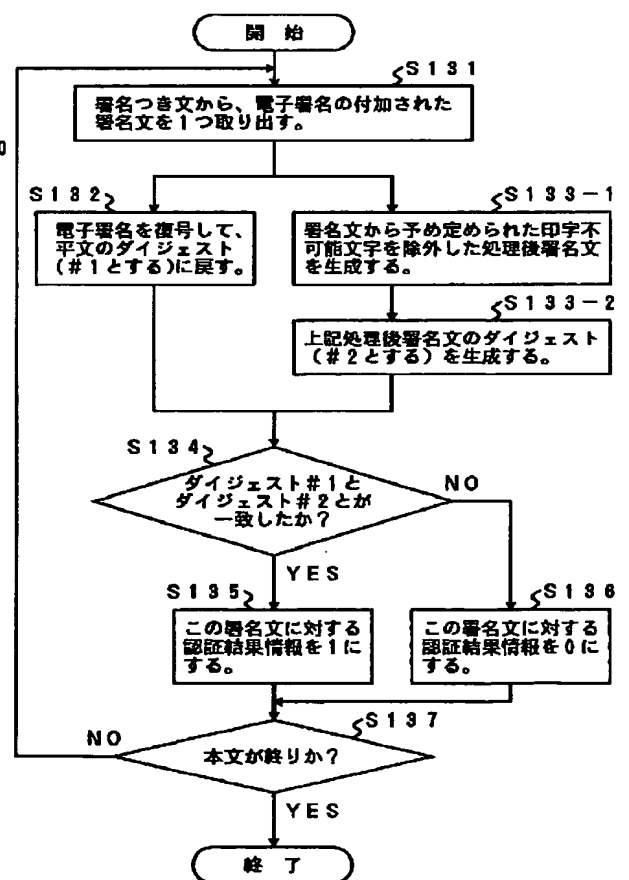
【図12】



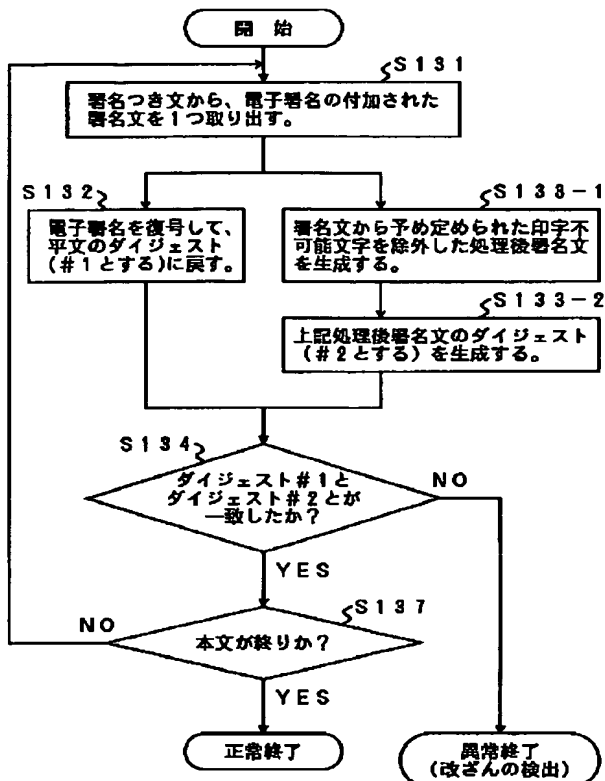
【図19】



【図13】



【図14】



【図16】

```

#define ILL_CHARS (34)
double tTrustND(m, k, l)
int m; /* ダイジェストに有効な文字数 */
int k; /* ダイジェストに無効な文字数 */
int l; /* ダイジェストのビット長 */
{
    int i;

    double mdlimit = pow(2.0, (double)l);
    double var = 1;

    for (i=1; i<k+1; i++)
        var = var*ILL_CHARS*(m+i);

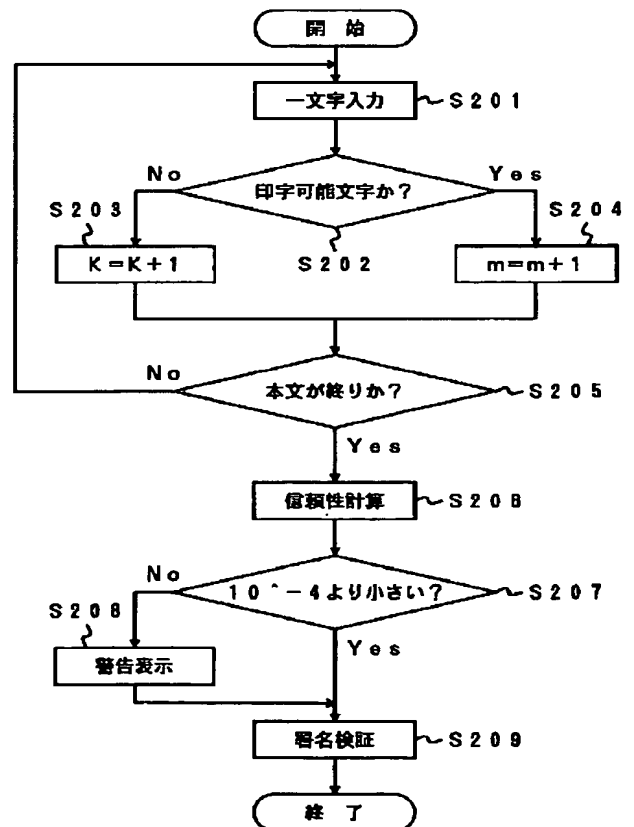
    return var/mdlimit;
}
  
```

【図15】

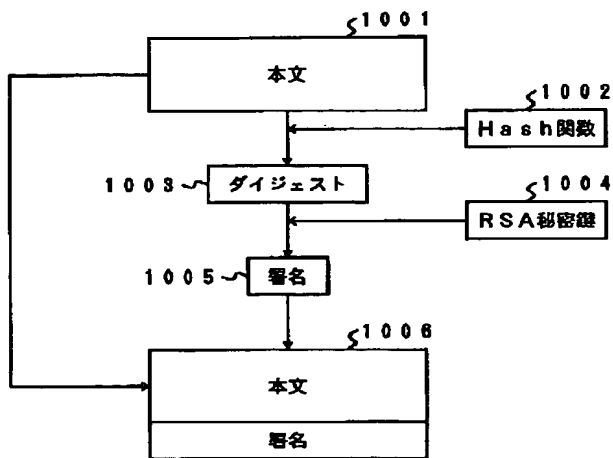
信頼性レベル=0.000100とした最大無効文字数

	ダイジェストのビット長			
有効文字数	32	64	128	256
2 ¹	2	6	14	27
2 ²	2	6	13	26
2 ³	2	5	12	25
2 ⁴	2	5	11	24
2 ⁵	1	4	11	23
2 ⁶	1	4	10	21
2 ⁷	1	4	9	19
2 ⁸	1	3	8	18
2 ⁹	1	3	8	17
2 ¹⁰	1	3	7	16
2 ¹¹	1	3	7	15
2 ¹²	1	2	6	14
2 ¹³	1	2	6	13
2 ¹⁴	0	2	6	12
2 ¹⁵	0	2	5	12
2 ¹⁶	0	2	5	11
2 ¹⁷	0	2	5	10
2 ¹⁸	0	2	4	10
2 ¹⁹	0	2	4	10

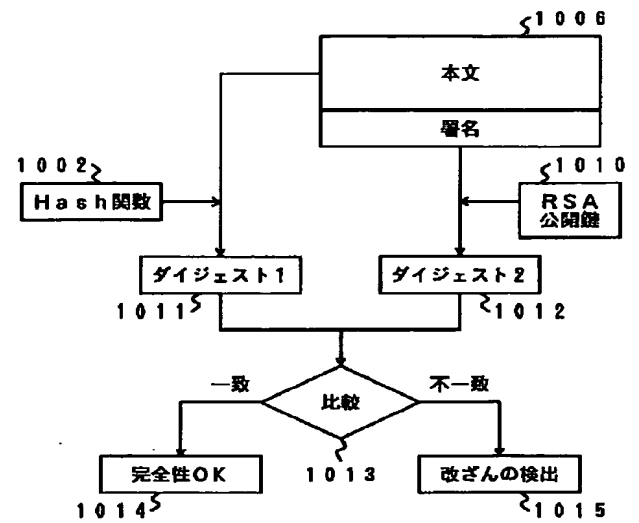
【図18】



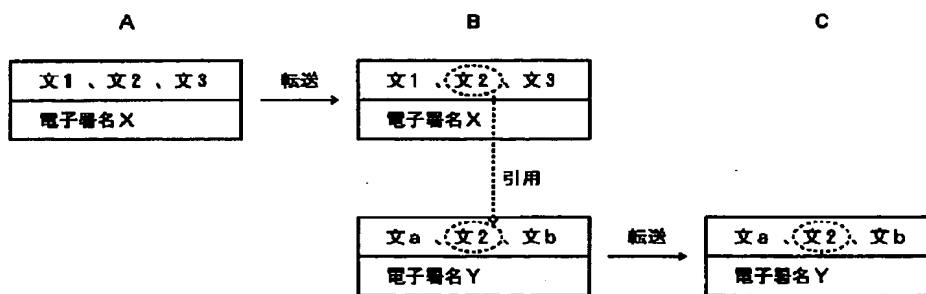
【図20】



【図21】



【図22】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.